



# New Features in Cloud-Delivered Firewall Management Center 2025

- [August 14, 2025, on page 1](#)
- [July 03, 2025, on page 3](#)
- [March 13, 2025, on page 3](#)

## August 14, 2025

Table 1: Features in Version 20250725

Feature	Minimum Threat Defense	Details
Zero Trust Access		
Universal Zero Trust Network Access (universal ZTNA).	7.7.10	<p>Universal Zero Trust Network Access (universal ZTNA) is a comprehensive solution that provides secure access to internal network resources based on user identity, trust, and posture. It ensures that access to one application does not implicitly grant access to the entire network, as with remote access VPN.</p> <p>New/modified screens: <b>Policies &gt; Zero Trust Application</b></p> <p>Requires Cisco Secure Access and Security Cloud Control.</p> <p>Deployment restrictions: Not supported with clustered devices, container instances, or transparent mode.</p> <p>Supported platforms: Secure Firewall 1150, 3100, 4100, 4200, and Firewall Threat Defense Virtual.</p> <p>See <a href="#">Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Security Cloud Control</a></p>
Administration		

Feature	Minimum Threat Defense	Details
Backup of Threat Defense devices.	Any	The Cloud-Delivered Firewall Management Center now retains only the five most recent Threat Defense device backups. All the older backups are deleted automatically.  See <a href="#">About Backup and Restore</a>
<b>Migration</b>		
Multi-instance Threat Defense device migration.	7.6	You can now migrate multi-instance Threat Defense devices that are part of a chassis, such as the Secure Firewall 3100/4200, to the Cloud-Delivered Firewall Management Center using the <b>Migrate FTD to cdFMC</b> feature in Security Cloud Control.  See <a href="#">Supported Features</a>
Migrate select Firepower 4100/9300 models to Secure Firewall 3100/4200.	<ul style="list-style-type: none"> <li>The source devices must be Version 7.2.x and later.</li> <li>The target devices must be Version 7.4.1 and later.</li> </ul>	<p>You can now easily migrate configurations to the Secure Firewall 3100/4200 from these devices:</p> <ul style="list-style-type: none"> <li>Firepower 4110, 4120, 4140, 4150</li> <li>Firepower 9300: SM-24, SM-36, SM-44</li> </ul> <p>See <a href="#">Threat Defense Model Migration</a></p>
Multi-instance mode conversion in the Firewall Management Center for the Secure Firewall 3100/4200.	7.6.0	<p>You can now register an application-mode device to the Firewall Management Center and then convert it to multi-instance mode without having to use the CLI.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> <li><b>Devices &gt; Device Management</b>, then for a device, click <b>More</b> (⋮) &gt; <b>Convert to Multi-Instance</b></li> <li><b>Devices &gt; Device Management</b>, then select multiple devices and choose <b>Select Bulk Action &gt; Convert to Multi-Instance</b></li> </ul> <p>See: <a href="#">Convert a Device to Multi-Instance Mode</a></p>

## July 03, 2025

Table 2: Features in Version 20250604

Feature	Minimum Threat Defense	Details
<b>Troubleshooting</b>		
Cisco RADKit integration.	7.7.0	<p>Cisco RADKit integration allows Cisco TAC engineers to remotely connect with your deployment (including sudo access) for an enhanced troubleshooting experience. You control the appliances and duration of access. This also gives you and Cisco TAC access to diagnostic data and logs.</p> <p>New/modified screens: <b>Devices &gt; Remote Diagnostics &gt; Enable the RADKit service</b></p> <p>See: <a href="#">Troubleshooting</a></p>

## March 13, 2025

Table 3: Features in Version 20250219

Feature	Minimum Threat Defense	Details
<b>Platform</b>		
Threat defense Version 7.7.0 support.	7.7.0	You can now manage threat defense devices running Version 7.7.0.
Secure Firewall 1230, 1240, and 1250 (rack-mount).	7.7.0	<p>We introduced the Secure Firewall CSF-1230 and CSF-1240:</p> <ul style="list-style-type: none"> <li>• 8x1Gbps RJ-45 1000BASE-T/2.5GBASE-T copper</li> <li>• 4x1Gbps SFP+ optical</li> </ul> <p>And the Secure Firewall CSF-1250:</p> <ul style="list-style-type: none"> <li>• 8x2.5Gbps 1000BASE-T/2.5GBASE-T copper</li> <li>• 4x2.5Gbps SFP28 optical</li> </ul> <p>See: <a href="#">Cisco Secure Firewall CSF-1230, CSF-1240, and CSF-1250 Hardware Installation Guide</a></p>

Feature	Minimum Threat Defense	Details
Optical transceivers for the Secure Firewall 4200.	7.7.0	<p>The Secure Firewall 4200 now supports these optical transceivers on the FPR4K-X-NM-2X200/400G network module: QDD-400G-DR4-S, QDD-4x100G-FR-S, QDD-4x100G-LR-S, QDD-400G-SR4.2-BD, QDD-400G-FR4-S, QDD-400G-LR4-S, QDD-400-CUxM, QDD-400-AOCxM, QDD-2X100-LR4-S, QDD-2X100-SR4-S, QDD-4ZQ100-CUxM.</p> <p>See: <a href="#">Cisco Secure Firewall 4215, 4225, and 4245 Hardware Installation Guide</a></p>
Secure Firewall 1210CP IEEE 802.3bt support (PoE++ and Hi-PoE).	7.7.0	<p>We made the following improvements related to support for IEEE 802.3bt:</p> <ul style="list-style-type: none"> <li>• PoE++ and Hi-PoE—Up to 90W per port.</li> <li>• Single- and dual-signature powered devices (PDs).</li> <li>• Power budgeting is done on a first-come, first-served basis.</li> <li>• Power budget fields were added to <b>show power inline</b>.</li> </ul> <p>New/modified screens: <b>Devices &gt; Device Management &gt; Interfaces &gt; PoE</b></p> <p>New/modified commands: <b>show power inline</b></p> <p>See: <a href="#">Regular Firewall Interfaces</a>, <a href="#">Cisco Secure Firewall Threat Defense Command Reference</a>.</p>
Instances for AWS, Azure, and GCP.	7.7.0	<p>We added instances for and Firewall Threat Defense Virtual from the following families:</p> <ul style="list-style-type: none"> <li>• AWS (Amazon Web Services): C6i and C6a</li> <li>• Azure (Microsoft Azure): Dv4 and Dv5</li> <li>• GCP (Google Cloud Platform): E2, N1, N2D, C2D</li> </ul> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Virtual Getting Started Guide</a></p>
<b>Device Management</b>		

Feature	Minimum Threat Defense	Details
Recovery-config mode for emergency on-device configuration and out-of-band configuration detection on the Firewall Management Center.	7.7.0	<p>If you lose the management connection to your device, you can make select configuration changes directly at the device CLI to:</p> <ul style="list-style-type: none"> <li>• Restore the management connection if you are using a data interface for manager access.</li> <li>• Make select policy changes that can't wait until the connection is restored.</li> </ul> <p>After the management connection is restored, the Firewall Management Center will detect the configuration changes on the device. It does not automatically update the device configuration in the Firewall Management Center; you must view the configuration differences, acknowledge that the device configuration is different, and then manually make the same changes in the Firewall Management Center before you deploy.</p> <p>New/modified screens: <b>Devices &gt; Device Management &gt; Device &gt; Health &gt; Out of Band Status</b></p> <p>New/modified diagnostic CLI (<b>system support diagnostic-cli</b>) command: <b>configure recovery-config</b></p> <p>See <a href="#">Device Settings</a>, <a href="#">Cisco Secure Firewall Threat Defense Command Reference</a></p>
<b>Interfaces</b>		
<b>Sync Device</b> is now <b>Sync Interfaces</b> .	Any	<p><b>Sync Device</b> was changed to <b>Sync Interfaces</b> to indicate that this function is only for interface changes. This function no longer detects changes made to the manager access interface; see <b>Devices &gt; Device Management &gt; Device &gt; Management &gt; Manager Access Details: Configuration</b>.</p> <p>Other out-of-band configuration changes performed at the diagnostic CLI in recovery-config mode need to be discovered at <b>Devices &gt; Device Management &gt; Device &gt; Health &gt; Out of Band Status</b>.</p> <p>New/modified screens: <b>Devices &gt; Device Management &gt; Interfaces</b></p> <p>See: <a href="#">Interfaces</a></p>
<b>High Availability/Scalability</b>		
Threat defense high availability supported with redundant manager access data interfaces.	7.7.0	<p>You can now use redundant manager access data interfaces with Firewall Threat Defense high availability.</p> <p>See: <a href="#">High Availability</a></p>
Autoscale for Firewall Threat Defense Virtual for Azure clusters.	7.7.0	<p>We now support autoscale for new Firewall Threat Defense Virtual for Azure clusters. You cannot convert upgraded deployments.</p> <p>Platform restrictions: Not supported with FTDv5 or FTDv10.</p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Virtual Getting Started Guide</a></p>
<b>VPN: Remote Access</b>		

Feature	Minimum Threat Defense	Details
Geolocation-based RA VPN.	7.7.0	<p>You can now allow or block remote access VPN connections based on country or region. Connections that don't meet your location-based criteria are blocked before authentication and logged for auditing purposes.</p> <p>New/modified screens: <b>Objects &gt; Object Management &gt; Access List &gt; Service Access</b></p> <p>See: <a href="#">Remote Access VPN</a></p>
Easily configure posture assessment criteria for dynamic access policies.	7.2.0	<p>In dynamic access policies (DAP), you can now easily configure <i>posture assessment criteria</i>—that is, file, process, or registry endpoint attributes with unique endpoint IDs that you can then use to configure DAP records.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> <li>• <b>Devices &gt; Dynamic Access Policy &gt; Add/Edit Policy &gt; Posture Assessment Criteria</b></li> <li>• <b>Devices &gt; Dynamic Access Policy &gt; Add/Edit Policy &gt; Add/Edit DAP Record &gt; Advanced &gt; Endpoint Criteria</b></li> </ul> <p>See: <a href="#">Dynamic Access Policies</a></p>
<b>Routing</b>		
BGP AS-Override.	7.7.0	<p>Firewall Threat Defense can now overwrite an ASN received from a peer with its own BGP ASN. This allows other routers peering with Firewall Threat Defense to accept advertised prefixes without detecting a loop based on the contents of the AS_PATH attribute.</p> <p>New/modified screens: <b>Devices &gt; Device Management &gt; Add/Edit Device &gt; Routing &gt; BGP IPv4 or IPv6 &gt; Add/Edit Neighbor &gt; AS Override</b></p> <p>See: <a href="#">BGP</a></p>
<b>Access Control: Threat Detection and Application Identification</b>		
Easily block traffic based on TLS version and server certificate status.	7.7.0	<p>New options in the decryption policy wizard make it easier to block traffic based on TLS version and server certificate status. Enabling these options adds predefined rules that do this. After the policy is created, you can edit, reorder, or delete the rules.</p> <p>New/modified screens: <b>Policies &gt; Decryption &gt; Create Decryption Policy &gt; Blocking</b></p> <p>See: <a href="#">Decryption Policies</a>, <a href="#">Decryption Rules</a></p>

Feature	Minimum Threat Defense	Details
Use EVE to easily bypass decryption for low-risk connections to trusted URLs.	7.7.0	<p>A new Client Threat decryption rule condition and a new option in the decryption policy wizard and make it easier to bypass decryption to trusted URLs for low risk (as identified by EVE) connections.</p> <p>New decryption policies now include predefined rules that do this, using Category (trusted) and Client Threat (low) conditions. The Client Threat condition is new and represents the EVE verdict. For outbound decryption, you enable/disable these rules as part of creating the policy. For inbound decryption, the rules are disabled by default. After the policy is created, you can edit, reorder, or delete the rules.</p> <p>New/modified screens: <b>Policies &gt; Decryption &gt; Create Decryption Policy &gt; Decryption Exclusions</b></p> <p>Version restrictions: You cannot deploy policies with Client Threat rules to older devices.</p> <p>See: <a href="#">Decryption Policies</a>, <a href="#">Decryption Rules</a></p>
New EVE exceptions.	7.7.0	<p>You can now bypass EVE (encrypted visibility engine) block verdicts based on source network and on destination dynamic attributes. And, when bypassing based on network, you can now use FQDN network objects. Previously, you could only block based on destination network or EVE process name and could not use FQDNs.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> <li>To add an exception from the access control policy, in the advanced settings, edit and enable <b>Encrypted Visibility Engine</b>, enable <b>Block Traffic Based on EVE Score</b>, and <b>Add Exception Rule</b>.</li> <li>To add an exception from the Unified Events viewer, right-click a connection that was blocked by EVE and select <b>Add EVE Exception</b>.</li> </ul> <p>See: <a href="#">Cisco Secure Firewall Management Center Snort 3 Configuration Guide</a></p>
<b>Access Control: Identity</b>		
Multicloud Defense connector for Cisco Secure Dynamic Attributes Connector.	Any	<p>The Multicloud Defense connector sends dynamic application address objects to the configured Cloud-Delivered Firewall Management Center.</p> <p>For more information, see the <a href="#">Address Objects</a> chapter in the <i>Cisco Multicloud Defense User Guide</i> and <a href="#">address object API documentation</a>.</p>
<b>Health Monitoring</b>		
Get alerts before service authentication certificates expire.	7.7.0	<p>To help prevent unexpected service disruptions, a new Certificate Monitoring health module alerts you before service authentication certificates expire on managed devices.</p> <p>New/modified screens: <b>System (⚙️) &gt; Health &gt; Policy &gt; Health Modules &gt; Certificate Monitoring</b></p> <p>See: <a href="#">Health</a></p>

Feature	Minimum Threat Defense	Details
Independently configure health monitoring for physical and subinterfaces.	Any	<p>You can now disable health monitoring for a physical interface while continuing to monitor and receive health alerts for its subinterfaces. You can disable alerts permanently or temporarily.</p> <p>To do this, configure the device for health monitoring exclusion, edit that configuration to enable module-level exclusion, and finally configure exclusion settings for the Interface Settings health module.</p> <p>New/modified screens: <b>System</b> (⚙️) &gt; <b>Health</b> &gt; <b>Exclude</b></p> <p>See: <a href="#">Health</a></p>
<b>Upgrade</b>		
Devices with internet access download upgrade packages from the internet.	Any (some restrictions)	<p>You can now begin device and chassis upgrades without the upgrade package. At the appropriate time, devices will get the package directly from the internet. This saves time and Firewall Management Center disk space.</p> <p>Devices without internet access can continue to get the package from the Firewall Management Center or an internal server. Note that devices try the internal server (if configured) before either the internet or the Firewall Management Center. If the internal server download fails, newer devices with internet access try the internet then the Firewall Management Center, while older devices and devices without internet access just try the Firewall Management Center. (In this context, "newer" means Firewall Threat Defense 7.6+ or chassis 7.4.1+.)</p> <p>Restrictions: Firewall Management Center and devices must be able to access the internet. There is no way to force a device with internet access to try the Firewall Management Center before it tries the internet. Not supported for hotfixes.</p> <p>Download location: <a href="https://cdo-ftd-images.s3-us-west-2.amazonaws.com/">https://cdo-ftd-images.s3-us-west-2.amazonaws.com/</a></p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center</a></p>



Feature	Minimum Threat Defense	Details
Upgrade Firewall Threat Defense or chassis without a manual readiness check.	7.7.0	<p>You no longer have to run time-consuming pre-upgrade readiness checks for Firewall Threat Defense or chassis upgrades. Instead, these checks are now regularly run by the system and reported in the health monitor. This allows you to preemptively fix any issues that will block upgrade.</p> <ul style="list-style-type: none"> <li>• The Database module, new for devices, manages monitors database schema and configuration data (<i>EO</i>) integrity.</li> <li>• The FXOS Health module, new for devices, monitors the FXOS httpd service on FXOS-based devices.</li> <li>• The Disk Status module is now more robust, alerting on disk health issues reported by daily running of smartctl (a Linux utility for monitoring reliability, predicting failures, and performing other self-tests).</li> </ul> <p>Version restrictions: This feature is supported for upgrades <i>from</i> Version 7.7+. Devices running earlier versions still require the in-upgrade readiness check.</p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center</a></p>
<b>Administration</b>		
Cancel Firewall Threat Defense backups, view detailed backup status.	7.7.0	<p>The Message Center now displays detailed backup status for the Firewall Management Center and its devices. You can also cancel in-progress device backups.</p> <p>See: <a href="#">Backup/Restore</a></p>
Clear disk space utility.	7.7.0	<p>A new utility allows you to click to safely remove unneeded files such as old backups, content updates, and troubleshooting files. Low disk space can reduce performance, prevent upgrade, and increase the risk of accidentally deleting important files when trying to recover space.</p> <p>New/modified screens: We added a <b>Clear disk space</b> button to the Disk Usage widget on device health dashboards: <b>System</b> (⚙️) &gt; <b>Health</b> &gt; <b>Monitor</b>.</p> <p>See: <a href="#">Troubleshooting</a></p>
Send detailed Firewall Management Center audit logs to syslog.	Any	<p>You can stream configuration changes as part of audit log data to syslog by specifying the configuration data format and the hosts. The Firewall Management Center supports backup and restore of the audit configuration log.</p> <p>New/modified screens: <b>System</b> (⚙️) &gt; <b>Configuration</b> &gt; <b>Audit Log</b> &gt; <b>Send Configuration Changes</b></p> <p>See: <a href="#">System Configuration</a></p>
<b>Performance and Resiliency</b>		

Feature	Minimum Threat Defense	Details
Faster failover for high availability Firewall Threat Defense.	7.7.0	<p>With Firewall Threat Defense high availability failover, the new active device generates multicast packets for each MAC address entry and sends them to all bridge group interfaces, which prompts the upstream switches to update their routing tables. This task now runs asynchronously in the data plane, privileging critical failover tasks in the control plane. This makes failover faster, reducing downtime.</p> <p>See: <a href="#">High Availability</a></p>
High-bandwidth encrypted application traffic bypasses unnecessary intrusion inspection.	7.7.0	<p>Specific high-bandwidth encrypted application traffic now bypasses unnecessary intrusion inspection even if the connection matches an Allow rule. Intrusion rule (LSP) and vulnerability database (VDB) updates can change the applications bypassed but right now they are: AnyConnect, IPsec, iCloud Private Relay, QUIC (including HTTP/3), Webex Media, Secure RTCP.</p>
Configure Firewall Threat Defense autorecovery from block depletion using FlexConfig.	7.7.0	<p>To reduce downtime due to service disruption, a new fault manager monitors block depletion and automatically reloads devices when necessary. In high availability deployments, this triggers failover. Fault monitoring is automatically enabled on new and upgraded devices. To disable, use FlexConfig.</p> <p>New/modified FlexConfig commands:</p> <ul style="list-style-type: none"> <li>• <b>fault-monitor block-depletion recovery-action { none   reload }</b>            Specifying <b>none</b> turns off automatic reload, but does not turn off fault monitoring. For that, use <b>no fault-monitoring</b>.</li> <li>• <b>fault-monitor block-depletion monitor-interval seconds</b>            You can configure how long (in seconds) before the device reloads.</li> </ul> <p>New/modified Firewall Threat Defense CLI commands: <b>show fault-monitor block-depletion { status   statistics }</b></p> <p>Platform restrictions: Not supported for clustered devices.</p> <p>See: <a href="#">Troubleshooting</a></p>
<b>Troubleshooting</b>		
CPU profiler includes application identification statistics.	7.7.0	<p>The CPU profiler now includes application identification statistics. That is, you can now see the resources used by processing specific application traffic. After you enable CPU profiling, use the CLI to see results.</p> <p>New/modified CLI commands: <b>system support appid-cpu-profiling status</b>, <b>system support appid-cpu-profiling dump</b></p> <p>See: <a href="#">Troubleshooting</a>, <a href="#">Cisco Secure Firewall Threat Defense Command Reference</a></p>

Feature	Minimum Threat Defense	Details
New IP flow statistics.	7.7.0	<p>When collecting IP flow statistics from Firewall Threat Defense under the direction of Cisco TAC, a new <b>all</b> parameter logs additional statistics to the specified file: port, protocol, application, cumulative latency, and inspection time.</p> <p>New/modified commands: <b>system support flow-ip-profiling start flow-ip-file <i>filename</i> all { enable   disable }</b></p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Command Reference</a></p>
<b>Security and Hardening</b>		
Require the Message-Authenticator attribute in all RADIUS responses.	7.0.7 7.7.0	<p><b>Upgrade impact. After threat defense upgrade, enable for existing servers.</b></p> <p>You can now require the Message-Authenticator attribute in all RADIUS responses, ensuring that the threat defense VPN gateway securely verifies every response from the RADIUS server, whether for RA VPN or access to the device itself.</p> <p>The <b>RADIUS Server-Enabled Message Authenticator</b> option is enabled by default for new RADIUS servers. We also recommend you enable it for existing servers. Disabling it may expose firewalls to potential attacks.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> <li>• <b>Objects &gt; AAA Server &gt; RADIUS Server Group &gt; Add RADIUS Server Group &gt; Add RADIUS Server</b></li> <li>• <b>System (⚙️) &gt; Users &gt; External Authentication &gt; Add External Authentication Object (RADIUS)</b></li> </ul> <p>New CLI commands: <b>message-authenticator-required</b></p> <p>Version restrictions: Not supported with Version 7.0–7.0.6, 7.1.x, 7.2.0–7.2.9, 7.3.x, 7.4.0–7.4.2, 7.6.0.</p> <p>Other restrictions: This feature introduced a login bug where the Firewall Management Center treats the RADIUS Class attribute (25) as octets instead of a string, which can break role mapping and cause login failures. For a list of fixed releases, or a workaround if you cannot upgrade, see <a href="#">CSCwq03404</a>.</p> <p>See: <a href="#">Objects Management</a>, <a href="#">Platform Settings</a></p>
Limited user privileges for Threat Defense CLI Basic user.	7.7.0	<p>The scope of the Threat Defense CLI Basic user privilege is now limited to the following commands: dig, ping, traceroute. If you have created users with the Basic privilege, evaluate whether you need to change them to the Config privilege. You can change a user's privilege level using the <b>configure user access</b> command.</p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Command Reference</a></p>
<b>Deprecated Features</b>		

Feature	Minimum Threat Defense	Details
Deprecated: Snort 2.	7.7.0	<p><b>Upgrade impact. Cannot upgrade Snort 2 devices.</b></p> <p>Snort 2 is deprecated. You cannot upgrade a Snort 2 device to Version 7.7.0+. Although you can use a Version 7.7.0+ Firewall Management Center to manage older Snort 2 devices, you should still switch to Snort 3 for improved detection and performance.</p> <p>Deprecated CLI commands: <b>show snort counters</b>, <b>show snort preprocessor-memory-usage</b>.</p> <p>See: <a href="#">Cisco Secure Firewall Management Center Snort 3 Configuration Guide</a></p>
Deprecated: Access control policy legacy interface.	Any	<p>You can no longer use the legacy user interface for access control policies. If you were using it, you switch to the improved user interface.</p> <p>New/modified screens: <b>Switch to Legacy UI</b> toggle is removed</p>